IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Ho Keung, Tse.
Application Number : 08/587,448
Filing Date : 12/01/95
Group Art Unit : 2202
Examiner : Laufer, P

P.O.Box 54670,
North Point Post Office,
Hong Kong.

Hon. Commissioner of Patents and Trademarks, Washington, D.C. 20231,
Box AF.

Sir,

Appeal Brief(Substitute)

This is an appeal brief of the above-identified application, filed by the above-identified applicant.

Real Party in Interest

As I am the sole inventor and has no assignee, and I represent myself in the prosecution of this application, there is no other real party in interest other than me, i.e., Ho Keung, Tse. And, I will inform the Board of Appeals and Interferences as soon as possible if sometime later, there is another party I know become "real party in interest" .

Related Appeals and Interferences

There is no related appeals and interferences known to me at this point of time and which will directly affect or be directly affected by or have a bearing on the decision in the pending appeal. And, I will inform the Board of Appeals and Interferences as soon as possible if sometime later, I find any such related appeals and interferences.

-1-

Status of Claims

Originally, rejected claims 1-7, 9-21 are on appeal for reconsideration.

However, I withdraw claims 6, 7, 10, 14, 20 from appeal hereby.

Claims 1-5, 9, 11-13, 15-19, 21 are presented, of which claims 1, 12, 17 are independent, each of claims 2-5, 9, 11 depends directly or indirectly on claim 1, each of claims 13, 15-16 depends directly or indirectly on claim 12 and each of claims 18, 19, 21 depends directly or indirectly on claim 17.

Please note that only reconsideration on allowability of independent claims 1, 12, 17 are necessary, the other claims are dependent claims and should be allowable if their corresponding independent claims are allowable.

Status of Amendments after Final

All amendments after final rejection, including substitute specifications, are not entered.

Those amendments include Amendment proposals filed on Nov 3, 97, on Dec., 10, 97, on Dec.,19, 97 , on Feb., 13, 98 , on Feb.,17, 98 and on March 18, 98.

Those amendments also include amendment proposals dated Feb., 18, 98, dated Feb., 26, 98(the date is printed on the last page), and dated April, 4, 98(the date is printed on the last page).

Those amendments further include Substitute specifications filed on Feb., 13, 98 and Mar.,18, 98 not entered, for the reasons that "entry of them requires careful analysis". The substitute specifications are for overcoming the objection of Examiner in the First and Final Office actions, the Examiner require "A substitute specification in proper idiomatic English and in compliance with 37 C.F.R. 152 (a and b)". The Examiner is respectfully requested to consider entry of them, once the rejections of the claims is withdrawn.

Summary of invention

The present invention is directed to protection of software from being copied by its rightful user to someone else for an unauthorised use thereof (readable on original specification, P.1, under the heading "Background of the invention".).

The authorising software and identity software of claims 1, 12 ; and authorising software of claim 17, meet an existing standard so that they can be used on a computer which also meets that existing standard and without modification thereof (readable from the original specification, P.3, under the heading "Detailed description of the preferred embodiments", line 3, the "IBM PC" as readable thereon is a standard computer and software for to be used thereon are standard softwares.). The computer comprises no hardware specific to the rightful or authorised user of the authorising software, for directly or indirectly authorising use of other software which being protected from unauthorised use, thereon (readable on whole original specification, in particular, P.1, under the heading "Background of the invention", second paragraphs, "the present invention ... provide a software ...to replace the above-mentioned hardware ... and which would not be copied by its rightful user to someone else".).

The authorising software of claims 1, 12, 17(corresponding to the ES program as readable on the original specification, P.5, item 3.) being for, when executed, authorising the protected software to be used on the standard computer.

The identity software of claims 1, 2 or means of claim 17(corresponding to the EI program as readable on original specification, P.4, item 2.) is for providing identity information of the rightful or authorised user of the authorising software.

The identity information(corresponding to "encryption result" as readable on original specification, P.4, item 2, second paragraph.) being for to be authenticated by a remote computer in order for the remote computer to perform operation(s) for which the rightful or authorised user has to be responsible(corresponding to "use...the

-3-

encryption result...from the EI program as a user authorisation for payment to be made from a user account" as readable on original specification, P.4, item 2, last paragraph, lines 3-4.).

Claim 1, is directed to the authorising software as mentioned above, and in particular, specifies that the identity software has no effective protection against unauthorised use (as it is readable on original specification, P.2, third paragraph, lines 3-6, "the ES program is protected from being unauthorised copied by its rightful user to someone else lies on the fact that a user would not copy ...EI program which can provided the user's encrypted identity for using the user's account", it should be understood that the EI program can be used by that "someone else" to provide the user's encrypted identity for using the user's account, in other words, the EI program has no protection against unauthorised use.) and that use of protected software on the computer will be authorised if the identity software is determined as being present on the computer by the authorising software(readable on original specification, P.8, item 5, first paragraph).

Claim 12, is directed to a "software" comprising the identity software and the authorising software and, in particular, specifies that they are contained in that "software" in such a manner that the authorising software is prevented from being copied therefrom individually(readable on original specification, P.2, second paragraph, lines 1-3.) ; and that the identity software has no individual and effective protection, provided by execution of that "software", against unauthorised use (as it is readable on original specification, P.2, third paragraph, lines 3-6, "the ES program is protected from being unauthorised copied by its rightful user to someone else lies on the fact that a user would not copy ...EI program which can provided the user's encrypted identity for using the user's account", it should be understood that the EI program can be used by that "someone else" to provide the user's encrypted identity for using the user's account, in other words, the EI program has no protection against

-4-

unauthorised use.) ; and that the software which being protected from unauthorised use is purchased software (readable on original specification, P.1, under the heading "Field of the invention", in particular, line1, last word, "sold".).

Claim 17 is directed to the authorising software and, in particular, specifies that a same encryption algorithm used in the means for providing an identity information; exists in the authorising software and being accessible or when the authorising software being executed, usable by a user(readable on original specification, P.8, item 5, third paragraph- fourth paragraph.).

A) Whether independent claims 1, 12, 17 and their dependent claims unpatentable under 35 U.S.C. 112, second paragraph, as argued by the Examiner in the final office action, P.2, **item 2a** ?

    Ai) Examiner's argument

    Aii) Traverse of rejections of independent claim 1 and its dependent claims.

    Aiii) Traverse of rejections of independent claim 12 and its dependent claims.

    Aiv) Traverse of rejections of independent claim 17 and its dependent claims.

B) Whether independent claims 1, 12, 17 and their dependent claims unpatentable under 35 U.S.C. 112, second paragraph, as argued by the Examiner in the final office action, P.2, **item 2b** ?

    Bi) Examiner's argument

    Bii) Traverse of rejections of independent claim 1 and its dependent claims.

    Biii) Traverse of rejections of independent claim 12 and its dependent claims.

    Biv) Traverse of rejections of independent claim 17 and its dependent claims.

C) Whether independent claims 1, 12, 17 and their dependent claims unpatentable under 35 U.S.C. 102(e), as argued by the Examiner in the final office action, P.2, **item 3** ?

    Ci) Examiner's argument

    Cii) Whether Ananda's claimed invention contains material X ?

    Ciii) Traverse of rejections of independent claim 1 and its dependent claims.

    Civ) Traverse of rejections of independent claim 12 and its dependent claims.

    Cv) Traverse of rejections of independent claim 17 and its dependent claims.

D) Whether the identity software(claims 1, 12) or executable codes for performing an algorithm used for providing identity information(claim 17) is a material capable of being used for protecting software ?

Di) Definition of "material X"

Dii) Whether "material X" is capable of being used for protecting software ?

Grouping of claims

a) Each of rejected independent claims 1, 12, 17 are separately patentable, they do not stand or fall together. Dependent claims 2-5, 9, 11 are grouped with their independent claim 1. Dependent claims 13, 15, 16 are grouped with their independent claim 12. Dependent claims 18, 19, 21 are grouped with their independent claim 17 .

b) Whether for rejections under 35 U.S.C. 112, second paragraph, as readable on the Final Office Action, P.2, items 2a and 2b, and for rejections under 35 U.S.C. 102(e), as readable on the Final Office Action, P.2, item 3, independent claims 1, 12, 17 should not stand or fall together ?

Claims 1, 12, 17 each has a respective different subject matter, therefore, for rejections under 35 U.S.C. 102(e) they should not stand or fall together. Further, as in each of them, a respective different language is used to define their respective different subject matter, therefore, for rejections under 35 U.S.C. 112, second paragraph, each of them should also not stand or fall together. Their respective different subject matters, are as follows :

Claim 1 requires "use of protected software on a computer will be authorised if the identity software is determined as being present on the computer".

Claim 12, requires "the identity software and authorising software are contained in a software in such a manner that the authorising software is prevented from being copied therefrom individually".

-7-

Claim 17 requires "a same encryption algorithm used in a means for providing an identity information, exists in the authorising software and being accessible or when the authorising software being executed, usable by a user".

Thus, claims 1, 12, 17 should not stand or fall together.

Argument

A) Whether independent claims 1, 12, 17 and their dependent claims unpatentable under 35 U.S.C. 112, second paragraph, as argued by the Examiner in the final office action, P.2, **item 2a** ?

Ai) Examiner's argument

In the final office action, item 2a, claims 1-5, 9, 11-13, 15-19, 21 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

In support of the rejections, the Examiner states that, "The claims are full of grammatical errors and dangling clauses which make the scope of the claims, indeterminate."

Aii) Traverse of rejections of independent claim 1 and its dependent claims.

The rejections are respectfully traversed. Although there are grammatical errors and dangling clauses in independent claim 1, most of them are wrong use of prepositions and the subject matter of claim 1 is well defined or well understood, for reasons as follows :

In the appendix herein below, claim 1, the subject matter is readable on paragraph 4, lines 1,2, "use of said other software on said computer will be authorised if said identity software is determined as being present on said computer", it should be understood that the term "said computer" therein is referring to the standard computer, not the remote computer, because similar phrases are readable on the second

-8-

paragraph, "1) authorising other software which being protected from unauthorised use, to be used on said computer ; 2) determining the presence of an identity software on said computer " and it is very clear that the term "said computer" in the similar phrases is referring to the standard computer readable on first paragraph therein, not the remote computer which first appears on the third paragraph therein.

Further, the original specification only discloses, as readable from the original specification, P.4, second paragraph, enabling a running program used on a computer by executing the ES program(corresponding to the authorising software of claim 1) on that computer, thereby preventing that program from unauthorised use on that computer, the original specification does not disclose "enabling a running program on a remote computer by executing the ES program on a local computer and protecting a program from unauthorised use on a remote computer". Therefore, claim 1 should not be interpreted as requiring such a limitation, and the term "said computer" should be interpreted as equivalent to "said standard computer", not "said remote computer".

As the subject matter is well defined, therefore, this error and other grammatical errors and dangling clauses in claim 1 should be minor errors and is corrected in claim 1(Three times Amended) submitted herein under the heading "Appendix B".

Aiii) Traverse of rejections of independent claim 12 and its dependent claims.

The rejections are respectfully traversed. Although there are grammatical errors and dangling clauses in independent claim 12, most of them are wrong use of prepositions and the subject matter of claim 12 is well defined or well understood, for reasons as follows :

In the Appendix A herein below, claim 12, paragraph 3, in the phrase "authorising software ... authorising use of other software ... on said computer ", it should be readily understood that the term "said computer" is referring to the standard computer,

not the remote computer, because the term "said computer" is already being used in the claim to refer to the standard computer in paragraph 2, line 1, before the first appearance of "remote computer" in second paragraph, line 4, and as readable on paragraph 2, line 5 that, the term "said remote computer" is being used to refer to "the remote computer".

Further, the original specification only discloses, as readable from the original specification, P.4, second paragraph, enabling a running program used on a computer by executing the ES program(corresponding to the authorising software of claim 12) on that computer, thereby preventing that program from unauthorised use on that computer, the original specification does not disclose "enabling a running program on a remote computer by executing the ES program on a local computer and protecting a program from unauthorised use on a remote computer". Therefore, claim 12 should not be interpreted as requiring such a limitation, and the term "said computer" should be interpreted as equivalent to "said standard computer", not "said remote computer".

In the Appendix A herein below, claim 12, the subject matter is readable on paragraph 4, lines 1-3, "said identity software and said authorising software are contained in said software in such a manner that said authorising software is prevented from being copied therefrom individually", it should be understood that the term "said software" is referring to the "software" as readable on line 1, the first word. For the reason that, claim 12 specifies that, that "software" comprising the identity software and the authorising software.

Further, the original specification does not discloses including ES program(corresponding to the authorising software) or EI program(corresponding to the identity software) in a software other than the central program, therefore it should be very clear that "said software" and the "software" is the same software which corresponds to the central program of the original specification.

As the subject matter is well defined, therefore, this error and other grammatical errors and dangling clauses in claim 12 should be minor errors and is

corrected in claim 12(Three times Amended) submitted herein under the heading "Appendix B".

Aiv) Traverse of rejections of independent claim 17 and its dependent claims.

The rejections are respectfully traversed. Although there are grammatical errors and dangling clauses in independent claim 17, most of them are wrong use of prepositions and the subject matter of claim 17 is well defined or well understood, for reasons as follows :

In the Appendix A herein below, claim 17, last paragraph, it should be readily understood that the term "said computer" is referring to the standard computer, not the remote computer, because the term "said computer" is already being used in the claim to refer to the standard computer in first paragraph, last line, before the first appearance of "remote computer" in second paragraph, line 2 and as readable on paragraph 2, line 2 that, the term "said remote computer" is being used to refer to "the remote computer".

In the Appendix A herein below, claim 17, the subject matter is readable on the second paragraph, lines 1-4, "wherein a same algorithm used by ....usable by a user". It should be noted that, there is a missing phrase "executable codes for performing" after "wherein". Even so, it is still readable on the phrase that "a same algorithm ... exists in said authorising software ... when said authorising software being executed ...usable by a user", and it should be interpreted to such an extent that "there exists executable codes in the authorising software for to be used by user, to perform the encryption algorithm".

As the subject matter is well defined, therefore, this error and other grammatical errors and dangling clauses in claim 17 should be minor errors and is corrected in claim 17(Three times Amended) submitted herein under the heading "Appendix B".

Av) Applicant's request

As the respective subject matters of the independent claims 1, 12, 17 are well defined, for the reasons submitted above, the rejections of independent claims 1, 12, 17 and their dependent claims under 35 U.S.C. 112 second paragraph, as readable on the final office action, item 2a, should be withdrawn and are respectfully requested.

B) Whether independent claims 1, 12, 17 and their dependent claims unpatentable under 35 U.S.C. 112, second paragraph, as argued by the Examiner in the final office action, P.2, **item 2b** ?

Bi) Examiner's argument

In the final office action, item 2b, claims 1-5, 9, 11-13, 15-19, 21 are rejected as failing to define the invention in the manner required by 35 U.S.C. 112, second paragraph.

In support of the rejections, the Examiner states that "the claims replete with indefinite and functional or operational language" and also that "the structure which goes to make up the device must be clearly and positively specified" and further that " The structure must be organised and correlated in such a manner as to present a complete operative device" and further that "For examination purpose, the claimed invention is understood as a software method".

Bii) Traverse of rejections of independent claim 1 and its dependent claims.

The rejections are respectfully traversed.

The identity software of claim 1 is a **useful material** capable of affecting human being behaviour in such a way that it make a user tends to protect his/her identity software from being used by someone else. For details please refer to item **D** herein below.

Claim 1 presents an authorising software from which a software method comprising the steps of 1) determining the presence of material X on a computer, 2) authorising use of the protected software on a computer if material X is determined as being present on that computer ; is readable.

Thus, the requirement of 35 U.S.C. 112, second paragraph is being met by claim 1.

Biii) Traverse of rejections of independent claim 12 and its dependent claims.

The rejections are respectfully traversed. The Examiner incorrectly interpreted the invention as defined by claim 12 as a computer based device.

The identity software of claim 12 is a **useful material** capable of affecting human being behaviour in such a way that it make a user tends to protect his/her identity software from being used by someone else. For details please refer to item **Dii** herein below.

Claim 12 presents a "software" which is also a useful material because it comprises the authorising software and the identity software therein, and has a well-defined composition.

Thus, the requirement of 35 U.S.C. 112, second paragraph is being met by claim 12.

Biv) Traverse of rejections of independent claim 17 and its dependent claims.

The rejections are respectfully traversed. The Examiner incorrectly interpreted the invention as defined by claim 17 as a computer based device.

As discussed in item **Aiv**, third paragraph, claim 17 requires executable codes for performing an encryption algorithm. Those executable codes as a whole is a **useful material** capable of affecting human being behaviour in such a way that it make a user tends to protect his/her software containing those codes from being used by someone else, for details please refer to item **D** herein below.

-13-

Claim 17 presents an authorising software which is also a useful material because it includes executable codes for performing the encryption algorithm, and has a well-defined composition.

Thus, the requirement of 35 U.S.C. 112, second paragraph is being met by claim 17.

Bv) Applicant's request

As the rejections of 35 U.S.C. 112, second paragraph, as readable on the final office action, item 2b, is not applicable to my independent claims 1, 12, 17, for the reasons submitted above, the rejections should be withdrawn and are respectfully requested.

C) Whether independent claims 1, 12, 17 and their dependent claims unpatentable under 35 U.S.C. 102(e), as argued by the Examiner in the final office action, P.2, **item 3** ?

Ci) Examiner's argument

In the Final Office Action, P.2, claims 1-5, 9, 11-13, 15-19, 21 are rejected under 35 U.S.C. 102(e) as being anticipated by Ananda(`645).

In support of the rejections, the Examiner states, in the Final Office Action, P.2, item 3, that the arguments in my response to First Office Action filed on 18 Aug., 97 are not deemed to be persuasive for the reasons that :

a) "the rightful user make copies of ... software available" is probably the most prevalent form of unauthorised software distribution ; and

b) "claim 12 specifies purchase and rental of software program is (as disclosed by Ananda) is merely a time-limited purchase".

Cii) Whether Ananda's claimed invention contains material X ?

Please refer to item **Di** for the definition of material X.

Ananda, as readable on all the claims thereof, describes a method of securely renting software, and as readable on claim 1, merely teaches of permitting continuous execution of application software in a first computer if authorisation is obtained from a second computer continuously, and execution will be terminated if otherwise. Claim 11 claims a similar method and in particular, specifies a rental application comprising a header program for, when being executed, transmitting from the first computer a password verification request comprising a system time, to the second computer, and the second computer will return a dynamic password in response, and the header program terminates the rental application if the dynamic password received does not match another dynamic password it generated using that system time previously. And, the purpose of the invention is readable on col. 23, lines 44-53, "The invention enables ... monitor the time period when a particular application software is executed by a user .... record the pertinent information regarding the execution of application software .... for billing and accounting purpose".

There is **no software** in Ananda's claimed invention which can meet the requirement of identity software of claims 1, 12. There is also **no means** in Ananda's claimed invention which can meet the definition of means for providing identity information of claim 17, and consequently, no "user-usable executable codes for performing an algorithm used in such a means for providing identity information" in Ananda's claimed invention and this is required by claim 17, for details please refer to argument **Aiv,** third paragraph, herein above.

Ananda's claims merely mention of a password verification request comprising a system time and there has no description in Ananda's claims as to whether user's identity has to be authenticated and if it has to be, in what way this should be done.

-15-

Ciii) Traverse of rejections of independent claim 1 and its dependent claims.

The rejections are respectfully traversed.

Claim 1, as readable on "Summary of invention" and please also refer to item **Aii** for the discussion of grammatical errors and dangling clauses therein, is directed to an authorising software and, in particular, specifies that the identity software has no effective protection against unauthorised use and that use of protected software on a computer will be authorised if the identity software is determined as being present on that computer by the authorising software.

Thus, the present invention as defined by the claim 1, is directed to an authorising software which makes use of the capability of affecting human behaviour of the identity software, for which details will be discussed herein below in argument **D,** to protect other software, namely as, the authorising software itself and the "protected software", **by using the presence of identity software on a computer as a precondition for authorising use of "protected software" on that computer,** and thereby, discouraging a user from allowing other person(s) to use the "protected software" or providing **a functional copy of the authorising software** to other person(s), and this is neither disclosed or suggested or described by Ananda's claims.

Ananda merely describes a method of securely renting software by using a remote computer to monitor the time period when a particular application software is executed and there is no software in Ananda's claimed invention which can meet the requirement of identity software of claim 1. For details please refer to item **Cii** herein above.

It is respectfully submitted that, software is capable of being copied, and it is therefore **an important innovative feature** of the present invention as defined by the claim 1 that, to protect software, i.e., authorising software and "protected software" against software piracy, by means of another software, i.e., the identity software.

-16-

Civ) Traverse of rejections of independent claim 12 and its dependent claims.

The rejections are respectfully traversed.

Claim 12, as readable on "Summary of invention" and please also refer to item **Aiii** for the discussion of grammatical errors and dangling clauses therein, is directed to a "software" comprising the identity software and the authorising software and, in particular, specifies that they are contained in that "software" in such a manner that the authorising software is prevented from being copied therefrom individually; and that the identity software has no individual and effective protection, provided by execution of that "software", against unauthorised use ; and that the software which being protected from unauthorised use is purchased software.

Thus, the present invention as defined by the claim 12, is directed to a software which makes use of the capability of affecting human behaviour of the identity software, for which details will be discussed herein below in argument **D**, to protect other software, namely as, the authorising software and the "protected software", **by making the authorising software inseparable from the identity software** , and thereby, discouraging a user from allowing other person(s) to use the "protected software" or providing **a duplication copy of that "software"** to other person(s), and this is neither disclosed or suggested or described by Ananda's claims.

Ananda merely describes a method of securely renting software by using a remote computer to monitor the time period when a particular application software is executed and there is no software in Ananda's claimed invention which can meet the requirement of identity software of claim 12. For details please refer to item **Cii** herein above.

It is respectfully submitted that, software is capable of being copied, and it is therefore **an important innovative feature** of the present invention as defined by the claim 12 that, to protect software, i.e., authorising software and "protected software" against software piracy, by means of another software, i.e., the identity software.

It is respectfully submitted that, it is not readable on Ananda's document that "the rental of software program" as disclosed therein is "merely a time-limited purchase" as argued by the Examiner in the final office action P.2, item 3.

And, it is readable on the "OXFORD ENCYCLOPAEDIC ENGLISH DICTIONARY" that, "purchase" means "acquire by payment" or "buy", whereas "rent" means "payment for use of a service, equipment, etc.". Accordingly, rental of a program can only be regarded as a purchase of right of time-limited use thereof, and the ownership thereof is not being transferred. And, to purchase a program of limited using time or to purchase the right of time-limited use of a program(i.e. rent) are completely different, in the former case the purchaser obtains the ownership of the program, although it may not be usable after a predetermined period of time, and in the latter case, the purchaser merely obtains the right of limited use and should return the program to its owner thereafter.

Further, as readable on independent claims 1, 8, 11 of Ananda, the rental software will be terminated on a first/user computer if authorisation or the like is not obtained from a second/remote computer. In other words, whether a user can continue to use a rental software or not depends on whether the user can obtain further authorisations or the like from the second computer which being not under his/her control, and therefore, even if the claimed software was not being indicated as "rental", it could not be a purchased software because a owner should have the right to use his/her software without authorisation from other party.

Ananda patent, as discussed in argument Cii herein above, is directed to using the second computer to "monitor the time period when a particular application software is executed by a user .... for billing and accounting purpose", and there has no description in Ananda's claims which suggests or discloses that use of the software can be permitted without authorisation(s) from the second computer or the second computer should be under complete control of the user to provide the authorisation(s), so as to protect purchased software, and "protection of purchased software" as

required by claim 12 is not being met by Ananda.

Cv) Traverse of rejections of independent claim 17 and its dependent claims.

The rejections are respectfully traversed.

Please refer to "Summary of invention", and to item **Aiv**, third paragraph for the discussion of grammatical errors and dangling clauses therein, **claim 17** is directed to the authorising software and, in particular, specifies that executable codes for performing a same encryption algorithm used in a means for providing an identity information, exists in the authorising software and being accessible or when the authorising software being executed, usable by a user.

Thus, the present invention as defined by the claim 17, is directed to an authorising software which makes use of the capability of affecting human behaviour of material X, i.e., the executable codes for performing the encryption algorithm used in the means for providing identity information, for which details will be discussed herein below in argument **D**, to protect other software, namely as, the authorising software and the "protected software", **by requiring user-usable executable codes for performing the encryption algorithm, exists in the authorising software,** and thereby, discouraging a user from allowing other person(s) to use the "protected software" or **providing a duplication copy of the authorising software** to other person(s), and this is neither disclosed or suggested or described by Ananda's claims.

Ananda merely describes a method of securely renting software by using a remote computer to monitor the time period when a particular application software is executed and there is no means in Ananda's claimed invention which can meet the definition of means for providing of claim 17. For details please refer to item **Cii** herein above.

Thus, no software of Ananda can meet the requirement of claim 17 that, "executable codes for performing a same encryption algorithm used in the means for providing an identity information, exists in ... software".

-19-

It is respectfully submitted that, software is capable of being copied, and it is therefore **an important innovative feature** of the present invention as defined by the claim 17 that to protect software, i.e., authorising software or "protected software" against software piracy, by means of another software, i.e., executable codes for performing the encryption algorithm.

Cvi) Applicant's request

As the present invention as defined by independent claims 1, 12, 17 is not anticipated or disclosed or suggested by Ananda's claims, for reasons submitted herein above, withdrawal of the rejections of independent claims 1, 12, 17 and their dependent claims under 35 U.S.C. 102(e) as being anticipated by Ananda(`645) are respectfully requested.

D) Whether the identity software(claims 1, 12) or executable codes for performing an algorithm used for providing identity information(claim 17) is a material capable of being used for protecting software ?

Claim 17 should be interpreted as requiring "user-usable executable codes for performing an algorithm used for providing identity information", for details please refer to argument **Aiv,** third paragraph, herein above.

Di) Definition of "material X"

Please note that, in order to simplify the argument, the identity software(claims 1, 12) or user-usable executable codes for performing an algorithm used for providing identity information(claim 17) will be referred to as **"material X"** herein below.

Dii) Whether "material X" is capable of being used for protecting software ?

It should be noted that, although material X is capable of being used for providing identity information of a user, for causing operation(s) for which that user has to be responsible, as required by claims 1, 12, 17, it is actually being used by the present invention as defined by the claims, for affecting human behaviour.

Specifically, as the identity information of a user is for causing operation(s) the user has to be responsible for, therefore a user in general will not copy or provide his/her identity software with no effective protection against unauthorised use (claim 1) or identity software with no individual and effective protection against unauthorised use(claims 12) or software containing user-usable executable codes for performing an algorithm used for providing identity information(claim 17) , i.e., material X, to someone else, in order to prevent himself/herself from having to take the responsibility of operation(s) caused by that someone else, even though the user may do this provided that both of them have a good enough relationship for he/she to do so.

It should be noted that, although the identity software of claim 12 may be protected against unauthorised use, it can not be protected individually, in other words, it has to be protected together with the authorising software because claim 12 is directed to a "software" comprising the identity software and authorising software, and therefore, unless the rightful user is willing to disable the protection of both the identity software and authorising software, an unauthorised user is incapable of using the authorising software.

Thus, material X is capable of being used as a **psychological barrier** to prevent that user from copying or providing itself or other material including software inseparable therefrom, to someone else.

In the past, **the Patent and Trademark Office** has shown that it **accepts** inventions which make use of **psychological barrier**, rather than physical barrier, to prevent unauthorised or illegal activities, **as useful** and can be patented. For instance, patent # : 5,437,323, entitled : Burglar deterrent decoy, it is readable on claim 1 that, "A burglar deterrent decoy comprises : a) a partial face mask with simulated eyes and nose ; ... mounting said partial face mask to a side jamb of a window ... behind a window blind ... retaining a slat of the window blind in front of said partial face mask in a bent up raised position so as to produce an illusion that a person is looking out through the window blind to scare away a burglar".
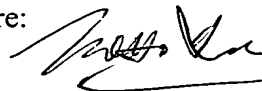
Requests

Should the Examiner or Board of Appeals disagree with the above, it is requested that it be indicated where, in the cited documents, there is a basis for such disagreement.

Date : June, 29, 98   Applicant : Ho Keung, Tse.

Signature:

1. Authorising software, stored in a device or physically on a medium, for use on a computer which being made to meet an existing standard such that any software product(s) meeting said standard can be used thereon and without modification thereof;

said authorising software being for, when executed, 1) authorising other software which being protected from unauthorised use, to be used on said computer; 2) determining the presence of an identity software on said computer;

said identity software being for use on said computer to, with no effective protection against unauthorised use, provide an identity information of the rightful or authorised user of said authorising software, said identity information being for to be authenticated by a remote computer in order for said remote computer to perform operation(s) for which said rightful or authorised user has to be responsible; and the presence of said identity software on said computer is being determined without a said operation being performed by said remote computer;

wherein use of said other software on said computer will be authorised if said identity software is determined as being present on said computer; and said authorising software and said identity software being software meeting said existing standard;

wherein said computer comprises no hardware specific to said rightful or authorised user for directly or indirectly authorising use of said protected software thereon.

2. Authorising software, stored in a device or physically on a medium, as claimed in claim 1, wherein comprising software, when being executed, for determining data integrity of said identity software; and if the determination is unfavourable, said identity software will further be determined as not present.

3. Authorising software, stored in a device or physically on a medium, as claimed in claim 1, wherein comprising authenticating software for, when being executed, authenticating said computer ; said authenticating software comprises a stored information of configuration of said computer and software for, when being executed, determining configuration of said computer and for comparing the determined result with said stored information ; and if the comparison result is unfavourable, said authorising software will not authorise use of said other software on said computer.

4. Authorising software, stored in a device or physically on a medium, as claimed in claim 3, wherein said configuration of said computer includes the hardware configuration thereof.

5. Authorising software, stored in a device or physically on a medium, as claimed in claim 3, wherein said configuration of said computer includes the software configuration thereof.

9. Authorising software, stored in a device or physically on a medium, as claimed in claim 1, wherein said other software comprises an information stored at a first predetermined location therein for indicating an valid identity of its rightful user exists at a second predetermined location therein and an encrypted identity of its rightful user at a respective location therein ; and said other software, when being executed, will fail to operate if said information therein being altered or said identity therein and said encrypted identity therein being inconsistent.

11. Authorising software, stored in a device or physically on a medium, as claimed in claim 9, wherein comprising an encrypted identity of its rightful user ; and if said other software stored in said computer has a valid user identity not consistent with said encrypted identity in said authorising software, said authoring software will not authorise use of said other software.

12. Software, stored in a device or physically on a medium, for use on a computer which being made to meet an existing standard such that any software product(s) meeting said standard can be used thereon and without modification thereof, comprising :

identity software for use on said computer to, with no individual and effective protection, provided by execution of said software, against unauthorised use, provide an identity information of the rightful or authorised user of an authorising software, said identity information being for to be authenticated by a remote computer in order for said remote computer to perform operation(s) for which said rightful or authorised user has to be responsible ;

said authorising software being for, when executed, authorising use of other software which being purchased and being protected from unauthorised use, on said computer ;

Wherein said identity software and said authorising software are contained in said software in such a manner that said authorising software is prevented from being copied therefrom individually ; and said authorising software and said identity software being software meeting said existing standard ;

wherein said computer comprises no hardware specific to said rightful or authorised user for directly or indirectly authorising use of said protected software thereon.

-25-

13. Software, stored in a device or physically on a medium, as claimed in claim 12, wherein said other software comprises an information stored at a first predetermined location therein for indicating a valid identity of its rightful user exists at a second predetermined location therein and an encrypted identity of its rightful user at a respective location therein ; and said other software, when being executed, will fail to operate if said information therein being altered or said identity therein and said encrypted identity therein being inconsistent.

15. Software, stored in a device or physically on a medium, as claimed in claim 13, wherein further comprising an encrypted identity of its rightful user ; and if said other software stored in said computer has a valid user identity which being not consistent with said encrypted identity in said software, said authorising software will not authorise use of said other software.

16. Software, stored in a device or physically on a medium, as claimed in claim 12, wherein said authorising software comprises said identity software.

17. Authorising software, stored in a device or physically on a medium and meeting an existing standard, for use on a computer which being made to meet said existing standard such that any software product(s) meeting said standard can be used thereon and without modification thereof ; said authorising software being for, when being executed, authorise other software which being protected from unauthorised use, to be used on said computer ;

wherein a same encryption algorithm used by a means for providing an identity information of the rightful or authorised user of said authorising software, exists in said authorising software and being accessible or, when said authorising software being executed, usable by a user ; said identity information being for to be authenticated by a remote computer in order for said remote computer to perform

operation(s) for which said rightful or authorised user has to be responsible ;

wherein said computer comprises no hardware specific to said rightful or authorised user for directly or indirectly authorising use of said other software thereon.

18. Authorising software, stored in a device or physically on a medium, as claimed in claim 17, wherein comprising authenticating software for, when being executed, authenticating said computer ; said authenticating software comprises a stored configuration information of said computer and software for, when being executed, determining configuration of said computer and comparing the determined result with said stored information ; and if the comparison result is unfavourable, said authorising software will not authorise use of said other software.

19. Authorising software, stored in a device or physically on a medium, as claimed in claim 17, wherein said other software comprises an information stored at a first predetermined location therein for indicating a valid identity of its rightful user exists at a second predetermined location therein and an encrypted identity of its rightful user at a respective location therein ; and said other software, when being executed, will fail to operate if said information therein being altered or said identity therein and said encrypted identity therein being inconsistent.

21. Authorising software, stored in a device or physically on a medium, as claimed in claim 19, wherein comprising an encrypted identity of its rightful user ; and if said other software stored in said computer has a valid user identity not consistent with said encrypted identity in said authorising software, said authorising software will not authorise use of said other software.

This is an amendment of claims 1, 12, 17, intended for eliminating the gramatical errors and dangling clauses in the claims and inwhich the original language of the claims is being used and not being changed.

1. (Third time amended) Authorising software, stored in a device or physically on a medium, for use on a computer (A) [which being made to meet] meeting an existing standard such that any software product(s) meeting said standard can be used thereon and without modification thereof ;

said authorising software being for, when executed, 1) authorising other software which being protected from unauthorised use, to be used on said computer (A) ; 2) determining the presence of [an] identity software [on] in said computer (A) ;

said identity software being for use on said computer (A) to , with no effective protection against unauthorised use, provide [an] identity information of the rightful or authorised user of said authorising software ;

said identity information being for to be authenticated by a remote computer (B) , in order for [said remote computer to perform] operation(s) for which said rightful or authorised user has to be responsible, to be performed by said remote computer (B) ; and the presence of said identity software [on] in said computer (A) is being determined without a said operation being performed by said remote computer (B) ;

wherein use of said [other] protected software on said computer (A) will be authorised if said identity software is determined as being present [on] in said computer (A) ; and said authorising software and said identity software being computer software meeting said existing standard ;

wherein said computer comprises no hardware specific to said rightful or authorised user for directly or indirectly authorising use of said protected software thereon.

-28-

12.(Third time amended) [Software] Protection software , stored in a device or physically on a medium, for use on a computer (A) [which being made to meet] meeting an existing standard such that any software product(s) meeting said standard can be used thereon and without modification thereof ;

said protection software comprising :

identity software for use on said computer (A) to , with no individual and effective protection , provided by execution of said software, against unauthorised use, provide [an] identity information of the rightful or authorised user of an authorising software ; said identity information being for to be authenticated by a remote computer (B) , in order for [said remote computer (B) to perform] operation(s) for which said rightful or authorised user has to be responsible, to be performed by said remote computer (B) ;

authorising software for, when executed, authorising use of other software which being purchased, and being protected from unauthorised use, on said computer (A) ;

Wherein said identity software and said authorising software are contained in said protection software in such a manner that said authorising software is prevented from being copied therefrom individually ; and said authorising software and said identity software being software meeting said existing standard ;

wherein said computer comprises no hardware specific to said rightful or authorised user for directly or indirectly authorising use of said protected software thereon.

17.(Third time amended) Authorising [software] program , stored in a device or physically on a medium and meeting an existing standard, for use on a computer (A) which [being made to meet] meets said existing standard such that any software product(s) meeting said standard can be used thereon and without modification thereof ;

-29-

said authorising [software] <u>program</u> being for, when [being] executed, [authorise] <u>authorising</u> other software which being protected from unauthorised use, to be used on said computer <u>(A)</u> ;

wherein <u>executable codes for performing an</u> [a same] encryption algorithm used by a means for providing [an] identity information of the rightful or authorised user of said authorising software, exists in said authorising [software] <u>program</u> and being accessible or, when said authorising [software] <u>program</u> being executed, usable by a user ;

said identity information being for to be authenticated by a remote computer <u>(B)</u> in order for [said remote computer to perform] operation(s) for which said rightful or authorised user has to be responsible, <u>to be performed by said remote computer (B)</u> ;

wherein said computer comprises no hardware specific to said rightful or authorised user for directly or indirectly authorising use of said other software thereon.